UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/834,084	04/11/2001	Michael S. Fox	42390P11074	2761

8791 7590 01/13/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/834,084	FOX ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 April 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☒ Claim(s) *1,10,19 and 25* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-28 have been examined and are pending.

Specification

The abstract of the disclosure is objected to because the applicant needs to make use of semi-colons to separate the items in a list or series when there are already other punctuation marks within the items themselves to make the abstract more easily understandable. Also, one of the items in the main series, which is itself a series, needs an "and" before concluding the last item in the sub-series.

1. Line 5: The comma after "code" should be a semi-colon.
2. Line 7: There should be an "and" before "the second database."
3. Line 8: The comma after "first database" should be a semi-colon.

Correction is required. See MPEP § 608.01(b).

The attempt to incorporate subject matter into this application by reference to http://www.sdmi.org (page 3, line 25 and page 6, line 25) is improper because the material disclosed by the reference is essential to the applicant's claims and should instead be submitted within an Information Disclosure Statement. As the material disclosed references a web site, there is no guarantee that the items the applicant thinks are relevant to his/her application will always be available or consistent.

The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code: http://www.sdmi.org (page 3, line 25 and page 6, line 25). Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Claim Objections

Claims 1, 10, 19, and 25 are objected to because of the following informalities:

1. Claim 1: There should be an "and" before "the second database" in line 7 to conclude the series.
2. Claim 10: The meaning of claim 10 is hard to follow as the applicant has lumped the features of the claim into one big paragraph instead of breaking the features up into a more readable format. The examiner recommends that the applicant break the features of claim 10 in a format similar to claim 1. In addition, the applicant need to use semi-colons where proper and needs to conclude a series with an "and" before the last item in the series:
    - Line 4: A semi-colon is needed between "database" and "by."
    - Line 5: A semi-colon is needed after "code."
    - Line 7: An "and" is needed before "the second database."
    - Line 8: A semi-colon is needed before "and."
3. Claim 19: The applicant needs an "and" before concluding the last item in a series and needs to remove an extra "and" as there are more items being listed in the series.
    - Line 9: An "and" is needed before "the second control database."
    - Line 15: The extra "and" needs to be removed. It appears that the applicant probably copied and pasted the line from a similar claim and forgot to remove the extra "and."
4. Claim 25: The applicant needs to remove the "and" in line 17.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 8, 10-18, and 25-28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 8 recites the limitation "the portion" in line 1. There is insufficient antecedent basis for this limitation in the claim. The examiner assumes the applicant meant "the portion of the first authentication code."
2. Claim 10 recites the limitation "the instructions" in lines 2 and 3. There are insufficient antecedent basis for these limitations in the claim. The examiner assumes the applicant meant "the plurality of machine readable instructions."
3. Claim 25 recites the limitation "the instructions" in lines 2 and 3. There are insufficient antecedent basis for these limitations in the claim.
4. Any claims not specifically addressed were rejected by virtue of dependency.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fox (U.S. 5,765,172) in view of "RFC 2104".

1. Claims 1 and 10: Fox discloses a method of, and an article comprising a storage medium having a plurality of machine readable instructions, wherein when the plurality of machine readable instructions are executed by a processor, the plurality of machine readable instructions provide for, deterring a rollback attack against a first database comprising:
    - Determining if the first database is corrupted, the first database being associated with a first authentication code (col 1, lines 65-67 and col 2, lines 1-6).
    - Determining if a second database is corrupted, the second database being associated with a second authentication code, and the second database having contents substantially the same as the first database (col 2, 2nd paragraph).

The examiner has interpreted an authentication code as any sort of hash, object, code, or checksum value associated with a database in any manner.

Fox does not teaches when the second database is not corrupted, recalculating the second authentication code using a portion of the first authentication code, copying the second database over the first database, and proceeding with authorized operations for processing content by an application program. However, RFC 2104 teaches the use of HMAC, (Key) Hashed Message Authentication Code. RFC 2104 discloses that an

authentication code using a hash or checksum, such as MD5, along with a secret key can be used to provide a way "to check the integrity of information transmitted over or stored in an unreliable medium" (RFC 2104, Introduction). One advantage of using HMAC over just an ordinary checksum algorithm is that the checksum algorithm portion of a HMAC can be replaced with a more secure or reliable algorithm discovered at a later date (RFC 2104, Introduction). Used in combination with the secret key, it is also more inherently secure than an ordinary checksum.

One of ordinary skill in the art at the time of the applicant's invention would be motivated to use HMAC instead of an ordinary checksum as an authentication code as this would inherently make the databases more secure, ensuring the integrity of the database as Fox was interested in doing. One of ordinary skill would also recognize that before copying the second database over the first, the second authentication code (which would also be transmitted to the first database) would have to be recalculated using the key portion of the first database's HMAC as the newly copied first database would need a new authentication code and its secret key is different than the second's secret key. Therefore, the newly calculated authentication code would have to use the first database's secret key in the calculation of a new code. After the corruption in the first database has been fixed, it is obvious to proceed with authorized operations for processing content by the application program as the error that caused it to stop in the first place has been fixed.

Claims 2-5 and 11-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fox (U.S. 5,765,172) in view of Stefik (U.S. 5,715,403) and "RFC 2104".

1. Claims 2 and 11: Fox does not teach the method of claim 1, when the second database is not corrupted, further comprising presenting a challenge code to a user of the application program, requiring the user to obtain a passcode in response to the challenge code, and determining the validity of the passcode, and performing the recalculating and copying only when the passcode is valid. However, Stefik teaches presenting a challenge code to a user of the application program, requiring the user to obtain a passcode in response to the challenge code, and determining validity of the passcode (col 3, lines 34-50). Stefik disclosed that it is possible for a user to have access to selected content already, but not be able to make any practical use of the content until they contact a central accounting facility to obtain a key/passcode to unlock the selected content. Stefik also discloses the use of a database to control usage rights (col 10, Table 1). Stefik does not teach the use of multiple databases to prevent a rollback attack (as seen in claim 1). However, as established already, Fox discloses the use of multiple databases to ensure database integrity and it would be obvious to one of ordinary skill in the art to copy the second database only when it is not corrupted and to make use of multiple databases as disclosed by Fox as this would give further control of usage rights. Further, it is obvious that since Stefik is interested in

the security of the digital content, to copy the database only when the passcode is also valid.

2. Claims 3 and 12: Fox discloses a method of claim 1 further comprising, and an article of claim 10, further comprising instructions for, continuing with authorized operations of the application program for processing content when the first database is not corrupted (col 7, lines 27-41 and fig 6). One of ordinary skill would recognize that there is no point in not doing anything if the first database is not corrupt and instead would continue with ordinary operations of the application.
3. Claims 4 and 13: Fox does not disclose the method of claim 1, wherein the first database comprises usage rules for processing selected content by the application program, the usage rules including a copy count for the selected content. This is, however, disclosed by Stefik (col 3, 1st paragraph; col 4, lines 4-24; and col 10 and 11, Table 1). One of ordinary skill in the art at the time of the applicant's invention would be motivated to combine the two teachings as Stefik was interested in controlling usage rights for digital content and the multiple database system disclosed by Fox would help achieve that goal.
4. Claims 5 and 14: Fox does not, but Stefik discloses the content comprising digital audio data (col 6, lines 48-52). Reasons one of ordinary skills would want to combine the two teachings have already been discussed.

Claims 6 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fox (U.S. 5,765,172) in view of Stefik (U.S. 5,715,403), "SDMI Portable Device Specification, Part 1, Version 1.0", and "RFC 2104".

1. Claims 6 and 15: Fox and Stefik does not specifically disclose the application program complying with requirements for a secure digital music initiative (SDMI) implementation. However, it would be obvious to one of ordinary skill in the art at the time of the applicant's invention that as one of the requirements of a SDMI application is that it "not violate Content Usage Rules," (p18, item 5.3.1 of "SDMI Portable Device Specification") one of ordinary skill in the art would use an application program which complies with SDMI as Stefik wants to not have the usage rules of the digital content disclosed with his invention violated.

Claims 7-9, 16-20, and 22-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fox (U.S. 5,765,172) in view of Stefik (U.S. 5,715,403) and "RFC 2104".

1. Claims 7 and 16: Fox does not teach a method and article of claims 1 and 10 respectively, wherein the first authentication code comprises a hash of the first database and a first secret, and the second authentication code comprises a hash of the second database and a second secret, the first secret being different than the second secret. However, as mentioned already, RFC 2104 discloses the use of HMAC, which uses a hash and a secret key, which are more secure than ordinary hashes or checksums.

Further it is obvious to use different secret keys for the first and second authentication code as this would make the databases further secure as should somehow a hacker were to break one authentication code, he/she would still need to spend some time to break the second.

2. Claims 8 and 17: It is obvious and inherent that if the first authentication code comprises a hash of the first database and a first secret, then a portion of the first authentication code would have to comprise the first secret.
3. Claims 9 and 18: Fox and Stefik does not specifically teach allowing a predetermined number of operations of copying the second database over the first database without presenting a challenge code to the user, requiring the user to obtain the passcode, and determining the validity of the passcode. However, it is obvious to one of ordinary skill in the art to have done so because the reason Stefik wanted to control the distribution and usage of digital content was so the owner can make a profit off the digital content. Stefik recognized that should the digital content user need to contact a central licensing facility for licensing issues all the time, someone would need to absorb the cost of communication—most likely the digital content owner (col 2, lines 44-54). Therefore, it makes sense to allow a predetermined number of copy operations of the second database over the first without presenting a challenge code to the user, as this would minimize the cost of running a central licensing facility.

4. Claims 19 and 25: Fox discloses a method of, and an article comprising a storage medium having a plurality of machine readable instructions, wherein when the plurality of machine readable instructions are executed by a processor, the plurality of machine readable instructions provide for:

   - Determining if the first database is corrupted, the first database being associated with a first message authentication code (MAC) (col 1, lines 65-67 and col 2, lines 1-6).
   - Determining if a second database is corrupted, the second database being associated with a second message authentication code (MAC), and the second database having contents substantially the same as the first database (col 2, 2nd paragraph).

The examiner has interpreted an authentication code as any sort of hash, object, code, or checksum value associated with a database in any manner.

Fox does not disclose, but Stefik teaches presenting a challenge code to a user of the application program, requiring the user to obtain a passcode in response to the challenge code, and determining validity of the passcode (col 3, lines 34-50). Stefik disclosed that it is possible for a user to have access to selected content already, but not be able to make any practical use of the content until they contact a central accounting facility to obtain a key/passcode to unlock the selected content. One of ordinary skill in the art at the time of the applicant's invention would be motivated to combine Stefik and Fox's teachings so that Stefik's invention would use at least two

databases to prevent a rollback attack against the first database in accordance with the teachings of Fox as Stefik is interested in controlling the distribution and usage of digital works through the use of his invention and a rollback attack would compromise this control. In the broadest reasonable interpretation, Table 1 as disclosed by Stefik (col 10 and 11) is a database, which is being used to keep track of usage and distribution rights. One of the items in the table/database is a field, which keeps track of the number of copies of a digital media in use (Table 1, 1st item). The number in this field is easily subject to a rollback attack.

Neither Fox nor Stefik teaches when the second database is not corrupted, recalculating the second MAC using a portion of the first MAC, copying the second database over the first database, and proceeding with authorized operations for processing content by an application program. However, RFC 2104 teaches the use of HMAC, (Key) Hashed Message Authentication Code. RFC 2104 discloses that an authentication code using a hash or checksum, such as MD5, along with a secret key can be used to provide a way "to check the integrity of information transmitted over or stored in an unreliable medium" (RFC 2104, Introduction). One advantage of using HMAC over just an ordinary checksum algorithm is that the checksum algorithm portion of a HMAC can be replaced with a more secure or reliable algorithm discovered at a later date (RFC, 2104, Introduction). Used in

combination with the secret key, it is also more inherently secure than an ordinary checksum.

One of ordinary skill in the art at the time of the applicant's invention would be motivated to use HMAC instead of an ordinary checksum as an authentication code as this would inherently make the databases more secure. One of ordinary skill would also recognize that before copying the second database over the first, the second authentication code (which would also be transmitted to the first database) would have to be recalculated using the key portion of the first authentication code's HMAC as the newly copied first database would need a new authentication code and its secret key is different than the second's secret key. Therefore, the newly calculated authentication code would have to use the first database's secret key in the calculation of a new code.

Fox discloses the use of multiple databases to ensure database integrity and it would be obvious to one of ordinary skill in the art to copy the second database only when it is not corrupted. Further, it is obvious that since Stefik is interested in the security of the digital content, to copy the database only when the passcode is also valid.

Fox discloses a method of claim 1 further comprising, and an article of claim 10, further comprising instructions for, continuing with authorized operations of the application program for processing content when the first database is not corrupted (col 7, lines 27-41 and fig 6). One of ordinary skill

would recognize that there is no point in not doing anything if the first database is not corrupt and instead would continue with ordinary operations of the application.

Fox does not teach, but Stefik discloses the first database comprising usage rules for processing selected content by the application program, the usage rules including a copy count for the selected content (col 3, 1st paragraph; col 4, lines 4-24; and col 10 and 11, Table 1).

Stefik further discloses the content comprising digital audio data (col 6, lines 48-52). After the corruption in the first database has been fixed, it is obvious to proceed with authorized operations for processing content by the application program as the error that caused it to stop in the first place has been fixed. As both databases essentially contain the same data, both databases are associated with the application program and both contain usage rules for the digital audio content.

The examiner would like to note that claim 19 is nothing more than a combination of claims 1-5 with some slight rewording of terms and that claim 25 is nothing more than a combination of claims 10-14 with some slight rewording of terms—i.e. "authentication codes" are called "message authentication codes" and "digital contents" are limited to "digital audio content" in the independent claim instead being limited to "digital audio content" by a later dependent claim.

5. Claims 20 and 26: Fox does not disclose, but Stefik teaches, a method of claim 19 and an article of claim 25, wherein the usage rules comprise a copy count for the digital audio content (col 6, Table 1, item 1). Motivations for combining the two teachings have been discussed already.
6. Claim 22 and 27: Fox does not teach a method and article of claims 19 and 25 respectively, wherein the first MAC comprises a hash of the first database and a first secret, and the second MAC comprises a hash of the second database and a second secret, the first secret being different than the second secret. However, as mentioned already, RFC 2104 discloses the use of HMAC, which uses a hash and a secret key, which are more secure than ordinary hashes or checksums. Further it is obvious to use different secret keys for the first and second MAC as this would make the databases further secure as should somehow a hacker were to break one MAC, he/she would still need to spend some time to break the second.
7. Claim 23 and 28: Fox and Stefik does not specifically teach allowing a predetermined number of operations of copying the second database over the first database without presenting a challenge code to the user, requiring the user to obtain the passcode, and determining the validity of the passcode. However, it is obvious to one of ordinary skill in the art to have done so because the reason Stefik wanted to control the distribution and usage of digital content was so the owner can make a profit off the digital content. Stefik recognized that should the digital content user need to contact a central

licensing facility for licensing issues all the time, someone would need to absorb the cost of communication—most likely the digital content owner (col 2, lines 44-54). Therefore, it makes sense to allow a predetermined number of copy operations of the second database over the first without presenting a challenge code to the user, as this would minimize the cost of running a central licensing facility.

8. Claim 24: Fox does not disclose, but Stefik teaches processing the digital audio content by an application program consistent with the usage rules (col 15, lines 17-29). Stefik does not teach a method of claim 19, wherein copying of the second control database over the first control database is performed after beginning execution of the application program but before proceeding with authorized operations. However, it is inherent that if Stefik's invention was to incorporate Fox's teachings to utilize two databases and to copy a second database onto a first database should the first database become corrupt, then the copying of the second database would not occur until after the beginning of the execution of the application program as the application program would check to verify the integrity of the database and authorized operations would not occur until the corruption has been fixed if one was detected, else there would be no point in attempting to detect the corruption.

Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fox (U.S. 5,765,172) in view of Stefik (U.S. 5,715,403) and "SDMI Portable Device Specification, Part 1, Version 1.0", and "RFC 2104".

1. Claim 21: Fox does not disclose the application program complying with requirements for a secure digital music initiative (SDMI) implementation. However, it would be obvious to one of ordinary skill in the art at the time of the applicant's invention that as one of the requirements of a SDMI application is that it "not violate Content Usage Rules," (p18, item 5.3.1 of "SDMI Portable Device Specification") one of ordinary skill in the art would use an application program which complies with SDMI as motivations have been established for combining Fox's and Stefik's teachings and Stefik wants to not have the usage rules of the digital content disclosed with his invention violated.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. Shin et al, "Hash Functions and the MAC Using All-or Nothing Property" discloses using hash functions in message authentication codes.
2. Kilner (U.S. 5,649,089) discloses maintaining multiple databases and using a checksum to ensure two databases are the same.
3. Lennie et al (U.S. 5,974,574) discloses maintaining replicated databases and using a checksum to ensure proper mirroring.
4. Wiser et al (U.S. 6,385,596) discloses the use of a digital passport.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100